Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 411 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 mei 2016

Mede namens de Ministers van Economische Zaken, Defensie, Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Veiligheid en Justitie, bied ik u hierbij de kabinetsreactie aan op het advies nr. 92 «Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht» van de Adviesraad Internationale Vraagstukken (AIV) en het advies nr. 94 «De publieke kern van het internet: naar een buitenlands internetbeleid» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).

De Minister van Buitenlandse Zaken,
A.G. Koenders

kst-26643-411
ISSN 0921 - 7371
’s-Gravenhage 2016

Kabinetsreactie op AIV advies «Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht» en WRR advies «De publieke kern van het internet: naar een buitenlands internetbeleid»

1. Inleiding

It is very difficult to make predictions, especially about the future
Niels Bohr, natuurkundige en Nobelprijswinnaar

De wereld wordt in steeds sneller tempo digitaal en het internet is de drijvende kracht achter deze ontwikkeling. Het internet genereert nieuwe kansen voor economische groei, innovatie en maatschappelijke ontwikkeling, maar zorgt ook voor nieuwe uitdagingen voor onze economie, veiligheid en vrijheid. Er wordt vaak gekeken naar de overheid om gepaste maatregelen te nemen om deze uitdagingen aan te gaan.

In de afgelopen periode verschenen diverse rapporten over de rol van de overheid ten aanzien van het internet. In december 2014 verscheen «Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht» (bijlage bij Kamerstuk 26 643, nr. 346) van de Adviesraad Internationale Vraagstukken (AIV), in maart 2015 volgde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) met «De publieke kern van het internet. Naar een buitenlands internetbeleid».

Het kabinet constateert dat Nederland al belangrijke stappen heeft gezet om maximaal te kunnen profiteren van de kansen die het internet biedt en ziet de rapporten van de AIV en de WRR als een aansporing om de ingezette koers te handhaven en te versterken. Dit vergt een robuuste nationale aanpak, gericht op het benutten van kansen die het internet biedt voor innovatie en economische groei en op het garanderen van veiligheid en mensenrechten in het cyberdomein. Het vergt ook een internationale cyberstrategie voor de omgang met kwesties rond de moeizame aansluiting van het internet – dat end-to-end open en grenzeloos is – op de bestaande internationale rechtsorde die is gebaseerd op een systeem van soevereine staten. De ontwikkeling van het internet vraagt om een voortdurende herijking van de bewegingsruimte en het handelingsperspectief van Nederland, zowel nationaal als internationaal. Het Nederlandse kabinet zet daarbij in op een vrij, open en veilig internet.

In deze brief reageert het kabinet op beide rapporten. Eerst wordt ingegaan op de uitdaging voor de overheid om haar handelen aan te passen aan de digitale realiteit. Daarnaast wordt in de algemene reactie op de analyse van de twee rapporten ingegaan op de drie hoofdthema's die de WRR en AIV behandelen: internet governance, veiligheid en mensenrechten. Tot slot, gaat deze brief in op de concrete aanbevelingen die worden gedaan in beide rapporten.

Deze reactie wordt namens het kabinet aangeboden door de Ministers van Buitenlandse Zaken, Economische Zaken, Defensie, en Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Veiligheid en Justitie.

2. Reactie op de analyse

De overheid staat continue voor de uitdaging haar handelen aan te passen aan de digitale werkelijkheid om ook in de toekomst te zorgen voor vrede, veiligheid en welvaart in Nederland én daarbuiten. Waar dit streven in de offline wereld uitdagingen creëert en belangenafwegingen vergt is dit ook

zo in de online wereld. Dat staten wereldwijd verschillend denken over het reguleren van het internet is daarom niet verrassend. Het kabinet zet in op een vrij, open en veilig internet waar maatschappelijke ontwikkeling, economische bedrijvigheid en innovatie de ruimte krijgen.

Een belangrijk begrip in het WRR rapport is de publieke kern van het internet, de kernprotocollen die het fundament vormen voor een goed functionerend internet, waaronder m.n. de zogenoemde internet protocol suite of TCP/IP suite. De AIV spreekt van het internet als een *mare liberum* waarbinnen de staat zich dient te beperken tot het borgen van de juridische kaders van de rechtstaat en het beschermen van de burgerlijke vrijheden. Het kabinet onderschrijft het belang van het behoud van het vrije en open karakter van het internet als platform voor onbelemmerd dataverkeer, ter stimulering van economische groei en innovatie. De *mare liberum*-vergelijking biedt goede aanknopingspunten, maar gaat niet volledig op omdat veiligheid en het respecteren van mensenrechten voorwaarden zijn voor economische groei en innovatie.

De overheid heeft de verantwoordelijkheid om haar burgers ook in een online omgeving te beschermen door de bescherming van hun persoonlijke informatie te bevorderen, cybersecurity te bevorderen en cybercriminaliteit en bedreigingen van de nationale veiligheid te bestrijden of te voorkomen. Internationale samenwerking wordt steeds belangrijker om deze belangen te beschermen in een grenzeloze digitale omgeving. Afspraken over samenwerking, (gedrags-)normen en standaarden moeten dan ook bij voorkeur in Europees en in breder internationaal verband worden gemaakt.

Bovengenoemde belangen vragen om een geïntegreerde benadering. In de optiek van het kabinet vormen vrijheid en veiligheid geen tegengestelde maar complementaire belangen. De dynamische balans tussen veiligheid, vrijheid en economische groei wordt tot stand gebracht en in stand gehouden in een constante open dialoog tussen alle stakeholders, zowel nationaal als internationaal. Deze visie op de samenhang tussen veiligheid, vrijheid en economische groei als basis voor beleidsafwegingen is verankerd in de Nationale Cyber Security Strategie 2.0[1]. De komende periode zal het kabinet een visie ontwikkelen voor het Nederlandse internationale cyberbeleid. Dit wordt in paragraaf 3.1 nader toegelicht.

Het kabinet benadrukt het belang van consistentie tussen binnenlands en buitenlands beleid. Enerzijds dienen de internationale standpunten van Nederland te volgen uit de nationale praktijk en is «preach what you practice» een uitgangspunt. Anderzijds leiden voorgenomen nationale maatregelen die afwijken van internationaal in te nemen standpunten en internationale verdragsverplichtingen tot een vermindering van geloofwaardigheid en effectiviteit bij het streven naar internationale ordening. In dat opzicht geldt ook «practice what you preach» als een uitgangspunt van nationaal beleid. Uiteraard geldt dat Nederland pas gehouden is aan internationale regelgeving als daarover internationaal overeenstemming is bereikt en Nederland de betreffende verplichting is aangegaan.

Internet Governance

Het kabinet onderschrijft de analyse van de AIV dat een open model van governance cruciaal is geweest voor de ontwikkeling van het internet. De WRR maakt onderscheid tussen de governance *van* het internet en

[1] «Nationale Cybersecurity Strategie 2.0: van bewust naar bekwaam», Nationaal Coördinator Terrorismebestrijding en Veiligheid, Bijlage bij Kamerstuk 26 643, nr. 291.

governance *die gebruik maakt van* het internet. Het kabinet zal ingaan op dit onderscheid en de rol van de staat in deze twee soorten governance. Besluiten over de verandering van de governance structuur van het internet kunnen grote invloed hebben op de manier waarop het internet zich als systeem in de toekomst verder zal kunnen ontwikkelen.

Nederland kiest voor een terughoudende opstelling ten aanzien van wat de WRR verstaat onder governance *die gebruik maakt van* het internet; het gebruiken van de internetinfrastructuur als instrument voor regulering van het beperken of beïnvloeden van de inhoudelijke aspecten van wat zich over het internet beweegt. Het uitgangspunt van het kabinet in dit verband is dat fundamentele rechten, zoals vrijheid van meningsuiting, online evenzeer van toepassing zijn als offline. Dit neemt niet weg dat de overheid ook op het internet onderzoek kan doen om deze vrijheden te borgen en criminaliteit te bestrijden, bijvoorbeeld om de verspreiding van haatzaaiende of discriminerende content op het internet te bestrijden.

Het Nederlandse internet governance beleid heeft tot doel de ontwikkeling, de openheid, de beschikbaarheid, de betrouwbaarheid en de integriteit van het internet te waarborgen. Het kabinet deelt de visie van de WRR en de AIV dat het huidige governance systeem heeft bewezen garant te staan voor een internetontwikkeling die bovenstaande aspecten weet te internaliseren. Om dit systeem in de toekomst te waarborgen, zal de rol van de technische gemeenschap, waaronder de Internet Engineering Taskforce (IETF) en het World Wide Web Consortium (W3C), behouden en versterkt moeten worden. Een belangrijk onderdeel daarvan is dat deelname in de besluitvorming over technische aspecten van het internet plaatsvindt op basis van kennis van die techniek en het vermogen om tot oplossingen te komen die de ontwikkeling van het internet ten goede komen, zonder dat hier politieke agenda's in meewegen.

Dankzij de effectieve vormen van zelforganisatie en zelfregulering die de open governance structuur van het internet kenmerken, is het internet uitgegroeid tot één wereldomspannende, gedeelde en toegankelijke infrastructuur. Daarbij is de multi-stakeholderaanpak effectief gebleken doordat zij de expertise van uiteenlopende stakeholders weet te benutten. De multistakeholder benadering sluit echter niet goed aan op het klassieke model van multilaterale onderhandelingen dat staten hanteren. In die zin is de kracht van het multistakeholder model ook zijn zwakheid: in zijn pure vorm werkt het model primair probleemoplossend, bijvoorbeeld in de manier waarop ingenieurs een technisch probleem oplossen. Er is echter geen overeenstemming over de verdeling van rollen en verantwoordelijkheden wanneer stakeholders bijeenkomen in verschillende internationale fora, wat kan schuren met de meer traditionele besluitvormingsmodellen. Dit bleek ook recentelijk weer tijdens de onderhandelingen over de eindverklaring van de *World Summit on Information Society (WSIS) +10 Review Process*, waar de zeer uiteenlopende visies op de rol van staten en andere stakeholders in de governance van het internet naar voren kwamen. In het slotdocument zijn op dit thema uiteindelijk alleen de beginselen uit de in 2005 overeengekomen Tunis Agenda herbevestigd: «We reiterate the working definition of Internet governance,[...], as the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet.»[2]

[2] «Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society», UN Doc. A/70/L.33, 13 December 2015, para. 58.

Het Internet Governance Forum (IGF) is het mondiale forum waar bovengenoemde partijen debatteren, informatie uitwisselen en proberen consensus te bereiken over de invulling van het governance model. Het IGF heeft echter geen mandaat om vervolgens hierover bindende besluiten te nemen. Er is in het internet governance domein behoefte aan verdere ontwikkeling en verbetering van de huidige modellen voor samenwerking en besluitvorming die staten en niet-statelijke actoren op een productieve wijze bij elkaar kunnen brengen. Hierbij kan niet automatisch worden teruggevallen op traditionele governance modellen, gezien de architectuur van het internet, het grote scala aan governance-onderwerpen en het grote aantal (technische, bestuurlijke en politieke) actoren dat daarbij betrokken is. Voor het IGF is het de komende jaren vooral de uitdaging dat het zich meer richt op tastbare en zichtbare resultaten,[3] nu haar mandaat met 10 jaar is verlengd.[4]

Het AIV- en het WRR-rapport gaan in op de rol van staten, vooral in de context van de Internet Corporation for Assigned Names and Numbers (ICANN). Dat is de Californische non-profit organisatie die operationele en coördinerende taken uitvoert voor een aantal (logische) functies van het internet en die besluit over de uitgifte van nieuwe internetdomeinen (zoals het domein.com). De ICANN-functies zijn zowel technisch, economisch, als politiek van groot belang en raken direct aan publieke belangen als de privacy van domeinnaamhouders, de bescherming van het intellectuele eigendom, (het verhogen van) de internetveiligheid en de naleving van mensenrechten. Daarnaast streeft ICANN naar het behoud van één ongefragmenteerd en open internet, een doelstelling waar het kabinet zich achter schaart.
Naar verwachting komt ICANN in de loop van 2016 los van het toezicht dat tot nu toe door de Amerikaanse overheid is uitgeoefend. Dit is een belangrijke stap in de sinds jaren door Nederland bepleite internationalisering van ICANN. Terecht benadrukt het AIV-rapport dat de toekomstige structuur van ICANN een belangrijk aandachtspunt van de regering moet zijn, gezien de implicaties voor lopende discussies over internet governance.

Nu ICANN autonoom doorgaat moet de verantwoordingsstructuur (accountability) binnen ICANN verbeterd worden en moet de overheidsrol in de voorgestelde nieuwe mechanismen opnieuw bepaald worden. In de discussie over het toekomstige toezicht op ICANN zijn er enerzijds staten die dat toezicht multilateraal willen beleggen bij de VN en anderzijds staten als Nederland, die inzetten op verdere uitbouw en versteviging van het bestaande multistakeholdermodel. Nederland pleit voor een actievere rol voor het comité van nationale overheden (verenigd in het Governmental Advisory Committee; GAC) bij besluiten van de ICANN Board, maar wil die wel beperkt houden tot adviserend. De multistakeholderopzet van de organisatie en de beslissingsbevoegdheid van het ICANN-bestuur mag niet worden ondermijnd of gepolitiseerd. Een wijziging van het systeem van internet governance mag niet ten koste gaan van de flexibiliteit, veiligheid en stabiliteit van het internet en van de bevordering van digitale rechten. Nederland is ervan overtuigd dat het internet het beste functioneert als alle belanghebbenden hun inbreng kunnen leveren en een rol kunnen spelen in het bestuur ervan. De huidige governnance praktijk heeft mede geleid tot de succesvolle ontwikkeling van het internet

[3] Daarover en over andere gewenste verbeteringen voor het IGF, o.a. wat betreft de deelname van relevante stakeholders uit ontwikkelingslanden, heeft een VN-werkgroep in 2012 aanbevelingen gedaan. De AVVN heeft in resolutie A/RES/68/198 van 20 december 2013 daarvan kennisgenomen.

[4] Krachtens AVVN-resolutie A/RES/70/125.

en de daaruit voortvloeiende economische en maatschappelijke voordelen.

Cybersecurity en andere vormen van veiligheid

Naast de vele kansen die het internet biedt voor economische groei en innovatie, creëert het ook uitdagingen voor de (nationale en internationale) rechtsorde en veiligheid. In paragraaf 3.3 zal het kabinet ingaan op de verschillende vormen van veiligheid die beide rapporten benoemen. In deze reactie op de algemene analyse wordt de veiligheidsuitdaging bezien vanuit de spanning tussen het internet als wereldwijd netwerk en de internationale rechtsorde die gebaseerd is op de soevereiniteit van nationale rechtsstaten.

Het internet wordt door kwaadwillende partijen misbruikt voor criminele activiteiten en acties die – ongeacht hun herkomst – ontwrichtende gevolgen kunnen hebben voor de Nederlandse samenleving.[5] Hier is sprake van een tweeledige internationale dimensie: buitenlandse actoren maken slachtoffers in Nederland en Nederlandse internetfaciliteiten worden gebruikt voor acties gericht op buitenlandse doelen. Het gaat daarbij om dreigingen die uitgaan van zowel statelijke als niet-statelijke actoren zoals cybercriminelen en terroristische bewegingen. De Nationale Cyber Security Strategie 2 beschrijft de visie op de taak en aanpak van de Nederlandse overheid in het voorzien van cybersecurity voor zijn burgers en bedrijven. Dit vindt plaats middels een geïntegreerde aanpak, die het verbeteren van kennis en inlichtingen over cyberdreigingen omvat, het opsporen van criminelen, het verhogen van de weerbaarheid, en de defensieve capaciteit en de opbouw van militaire capaciteiten, en actieve cyberdiplomatie.

Het grensoverschrijdende en mondiale karakter van het internet vereist dat uitdagingen die zich hier op het gebied van veiligheid voordoen internationaal aangepakt worden. Aangezien de internationale rechtsorde gebaseerd is op het principe van soevereiniteit kan de nationale overheid de veiligheidsuitdagingen op het internet slechts in beperkte mate eigenstandig ondervangen. Daarvoor is internationale samenwerking vereist, zoals binnen de EU, VN en Raad van Europa. Nederland draagt dan ook actief bij aan de internationale discussies en de versterking van de internationale rechtsorde. Dat neemt niet weg dat nog veel zaken die nationaal geregeld zijn internationaal nog uitgewerkt moet worden.

Bij de bestrijding van cybercrime werkt Nederland actief samen o.a. in het kader van de Boedapest Conventie, de EU (zoals bijvoorbeeld met Eurojust en Europol) en met INTERPOL. De bestrijding van cybercriminaliteit stelt nieuwe eisen aan met name de handelingssnelheid en informatie-uitwisseling van politie en justitie. Deze ontwikkelingen in het digitale domein kunnen ook een heroverweging van de juridische kaders vergen. Nederland is actief in de discussie over de effectiviteit van het internationaal juridisch kader voor grensoverschrijdende opsporing en onderzoek naar misdrijven in cyberspace en ontwikkelt zelf nieuwe instrumenten en wetgeving om het eigen handelingsperspectief te verbeteren. Het spreekt voor zich dat bij nieuwe wetgeving wordt getoetst aan internationaal rechtelijke verplichtingen. Het door de AIV aangehaalde conceptwetsvoorstel Computercriminaliteit III is inmiddels aan het parlement gestuurd.

[5] Cybersecuritybeeld Nederland 2015. (bijlage bij Kamerstuk 26 643, nr. 369).

Bescherming van de publieke kern van het internet

Het kabinet onderschrijft de notie van de WRR dat de economische en sociale voordelen van het internet afhankelijk zijn van het betrouwbaar, voorspelbaar, stabiel, en veilig functioneren van de kernprotocollen van het internet. Hierbij erkent het kabinet dat wat de WRR onder deze «publieke kern» verstaat, kenmerken vertoont van een internationaal publiek goed dat afzonderlijke soevereine en particuliere belangen overstijgt. Over wat precies onder deze publieke kern kan worden geschaard is het WRR rapport echter niet conclusief. Ook internationaal is hier geen overeenstemming over. Het kabinet neemt als uitgangspunt dat de kernprotocollen van het internet de publieke kern vormen.

Nederland erkent dat de aard en de afhankelijkheid van het digitale domein vragen om terughoudendheid ten aanzien van activiteiten die aan de publieke kern kunnen raken. Op zichzelf rechtmatige ingrepen van een staat kunnen schadelijke gevolgen hebben voor de publieke kern van het internet waar andere staten negatieve gevolgen van kunnen ondervinden.

Het kabinet zet er zich voor in dat de instandhouding en ontwikkeling van de «publieke kern» zoveel mogelijk blijft voorbehouden aan de technische gemeenschap en de statelijke rol zich zo veel mogelijk richt op de ondersteuning daarvan. Zoals hierboven beschreven waarborgt de huidige governance structuur een gedepolitiseerd proces dat gericht is op het oplossen van problemen en het faciliteren van de ontwikkeling van het internet in brede zin.

Daarnaast geldt dat het kabinet ook in cyberspace streeft naar het bevorderen van de internationale rechtsorde. De bescherming van de «publieke kern» is een kwestie van internationale veiligheid, in gevallen waarin cyberoperaties door statelijke of niet-statelijke actoren er toe kunnen leiden dat het functioneren van de publieke kern van het internet negatief kan worden beïnvloed.

Ondanks enkele concrete resultaten zoals de rapporten van de United Nations Group of Governmental Experts en de publicatie van de *Tallinn Manual on the International Law Applicable to Cyber Warfare*, bevindt het proces van internationale ordening zich in een vroeg stadium. De meeste aandacht gaat tot nu toe uit naar het beschermen van vitale infrastructuur op nationaal niveau, met name voor de ondersteuning van vitale civiele functies. Uitgangspunt daarbij is dat deze vitale infrastructuur beschermd wordt door het verbod op het gebruik van geweld en het verbod op de schending van de soevereiniteit van andere staten. Ook op grond van de principes en regels van het humanitair oorlogsrecht, mag een bepaalde bescherming van vitale, niet-militaire infrastructuren worden verwacht. Nederland zet zich actief in om de toepassing van het bestaande internationaal recht op cyberoperaties te verduidelijken en daarover tot brede overeenstemming te komen.

Het voorkomen en reguleren van cyberaanvallen is onderwerp van internationaal overleg en academisch onderzoek, dat zich richt op het verhelderen van de toepassing van het internationaal recht en het ontwikkelen van aanvullende gedragsnormen tussen staten. Door daarvoor een normatief kader te ontwikkelen, wordt geprobeerd om de handelingsruimte kleiner te maken voor kwaadwillende staten en niet-statelijke actoren die zich niet aan internationale afspraken houden, en om de internationale solidariteit te vergroten om dergelijke activiteiten te veroordelen. Het kabinet ziet dit als noodzakelijke eerste stappen naar meer internationale ordening in cyberspace.

Door de aard van het cyberdomein is het moeilijk verifieerbare afspraken te maken over het handelen van staten. Het ontwikkelen van breed gedragen gedragsnormen biedt echter wel mogelijkheden om ordening aan te brengen op basis van het gedeelde belang van een goed functionerend en betrouwbaar internet. Zulke gedragsnormen kunnen de politieke, diplomatieke en economische kosten voor het uitvoeren van schadelijke activiteiten verhogen. Een voorbeeld van zo'n gedragsnorm waarover recent consensus is bereikt in VN kader is de aanbeveling: «[A] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;»[6] Het kabinet beschouwt deze aanbeveling als een eerste aanzet voor het beschermen van infrastructuur, waaronder informatie-infrastructuur.

Nederland is actief betrokken bij de internationale discussie omtrent mogelijke gedragsnormen voor de bescherming van of zelfs non-interventie in (onderdelen van) de publieke kern van het internet en wil verder onderzoeken hoe dergelijke normen gerealiseerd kunnen worden. Daarnaast zal het kabinet onderzoeken of het mogelijk is om groepen met een belangrijke rol voor het onderhoud van het technische niveau beter te ondersteunen. Een voorbeeld daarvan is de open-source community, die veelal pro-deo werkt aan onderhoud, ontwikkeling en verdere uitbouw van belangrijke delen van de publieke kern van het internet. Het in een faciliterende rol financieel ondersteunen van de ontwikkeling valt onder deze noemer, met als concreet voorbeeld de steun voor versterking van encryptie via open source projecten.[7]

Digitale rechten en internetvrijheid

Ook op het gebied van rechten in het digitale domein manifesteren zich uitdagingen die een nationale overheid slechts ten dele kan ondervangen. De bescherming van mensenrechten in een online omgeving vereist internationale samenwerking binnen regionale en internationale organisaties.

De AIV behandelt in haar advies de belangrijkste thema's die de discussie over online rechten domineren: het recht op bescherming van privacy, de vrijheid van meningsuiting en de rol van de opsporingsdiensten. De ontwikkeling van het internet dwingt tot een heroriëntatie op juridische kaders die ontwikkeld zijn voor bescherming van rechten in een andere tijd met een andere stand van de techniek. Voor het kabinet is van belang dat de kernwaarden van de Nederlandse samenleving zoals vervat in de Nederlandse Grondwet en internationale mensenrechtenverdragen de juridische kaders vormen voor de borging van de mensenrechten in de digitale samenleving. Het kabinet streeft naar een adequate bescherming van deze grondrechten in het digitale domein en naar bevordering van toepassing van vergelijkbare standaarden in het internationaal recht.

Een voorbeeld is de gids met rechten van internetgebruikers van de Raad van Europa.[8] Een inbreuk op een grondrecht is alleen toegestaan als er een wettelijke basis voor is en indien voldaan wordt aan de minimumvereisten van proportionaliteit en noodzakelijkheid. Recente jurisprudentie

---

[6] «Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security», UNGA Doc. Nr. A/70/174, para. 13(f).

[7] https://zoek.officielebekendmakingen.nl/kst-34300-XIII-160.html. (Kamerstuk 34 300 XIII, nr. 160)

[8] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. Adopted by the Committee of Ministers on 16 April 2014. Zie http://www.coe.int/en/web/internet-users-rights/guide.

van het Europese Hof voor de Rechten van de Mens (EHRM) en het Europese Hof van Justitie met betrekking tot het digitale domein biedt aanknopingspunten voor de wijze waarop aan de eisen van noodzakelijkheid en proportionaliteit invulling kan worden gegeven, waaronder waarborgen met betrekking tot de aard, de reikwijdte en de duur van maatregelen die het recht op privacy inperken.[9] In de Nederlandse context is een inbreuk op deze grondrechten alleen mogelijk op basis van zwaarwegende maatschappelijke belangen, zoals het voorkomen, opsporen en vervolgen van misdrijven. Ook dient adequate rechtsbescherming open te staan voor individuen wiens grondrechten worden aangetast.

Ten aanzien van het werk van de inlichtingen- en veiligheidsdiensten heeft de Commissie Dessens[10] geconcludeerd dat de technologie enorm is veranderd in de voorbije tien jaar, waardoor een aanpassing van de Wet op de Inlichtingen en Veiligheidsdiensten (Wiv) op een (meer) techniek-onafhankelijke manier noodzakelijk is, in combinatie met een verstevigd kader van toestemmingsvereisten en toezicht. Het kabinet is voornemens deze tekortkoming door middel van een wetswijziging te herstellen, en de waarborgen voor de bescherming van de persoonlijke levenssfeer te versterken. Verdere bespreking van de herziene Wiv valt thans buiten de scope van deze brief, gezien dit proces van wetswijziging thans gaande is. Wel kan hier in reactie op de rapporten gesteld worden dat ook in dit proces de verschillende belangen zorgvuldig zullen worden afgewogen binnen de hierboven beschreven juridische kaders en in lijn met het streven van het kabinet naar een vrij, open en veilig internet.

3. Reactie op deeladviezen WRR

3.1 Naar een internationaal cyberbeleid

Zowel de AIV als de WRR pleiten ervoor om een geïntegreerde internationale cyberstrategie te formuleren. Het kabinet onderschrijft dit advies. Nederland heeft belang bij een geïntegreerde afweging van Nederlandse belangen op het gebied van het internet en een daarop gebaseerde internationale strategie die recht doet aan de verschillende belangen. De manier waarop Nederland keuzes maakt, is van directe invloed op de positionering van Nederland als gidsland, vestigingsland en partnerland.

Hoewel op verschillende beleidsterreinen reeds intensief wordt samengewerkt in internationaal verband, kan de afstemming *tussen* beleidsterreinen versterkt worden zodat een betere integrale afweging kan plaatsvinden. Op verschillende beleidsterreinen, waaronder cyber security en de digitale agenda, is een coördinatiestructuur opgezet voor standpuntbepaling en besluitvorming, waarin de Ministeries van Economische Zaken, Veiligheid en Justitie, Defensie, Buitenlandse Zaken en Binnenlandse Zaken en Koninkrijksrelaties actief participeren. De intensieve samenwerking tussen de ministeries is in de aanloop naar de Global Conference on Cyberspace in april 2015 al aanzienlijk versterkt. Het kabinet onderschrijft het belang van goede interdepartementale coördinatie om te komen tot een integrale afweging van Nederlandse belangen op het gebied van internet.

---

[9] Zie onder meer HvJ EU 8 april 2014, C-293/12 en C-594/12 (Digital rights Ireland t. Ierland); HvJ EU 6 oktober 2015, C-362/14 (Schrems t. Data protection Commissioner); EHRM 12 januari 2016, nr. 37138/14 (Szabó and Vissy t. Hongarije).

[10] (Kamerstuk 33 820, nr. 2).

Het kabinet zal de komende tijd werken aan een aanzet voor een geïntegreerde internationale cyberstrategie die complementair is aan en in lijn is met nationale beleidskeuzes op het gebied van cyber. De strategie brengt de internationale ontwikkelingen in kaart en geeft een afwegingskader voor de manier waarop Nederland internationaal optimaal zijn nationale doelstellingen kan realiseren. Hiervoor zal breed geconsulteerd worden bij diverse stakeholders. Zonder in de beleidsverantwoordelijkheid van de verschillende ministeries te treden, wordt gestreefd naar een visie die recht doet aan de verwevenheid van de verschillende thema's met betrekking tot het internet, zoals terecht aangegeven door de AIV en de WRR. Ook biedt de strategie de mogelijkheid om de Nederlandse inzet in verschillende internationale fora, zoals de VN, NAVO, OVSE, EU en Raad van Europa, beter af te stemmen. Daarnaast werkt het kabinet doorlopend aan de versterking van de structurele afstemming tussen departementen en uitvoeringsorganisaties, opdat de Nederlandse inzet in internationale fora altijd coherent, helder en effectief is.

Het kabinet is van mening dat het internationaal cyberbeleid gebaseerd dient te zijn op de nationale belangen van Nederland. Tegelijk wordt deze strategie ook gevoed door internationale ontwikkelingen, zowel op technologisch, internationaalrechtelijk, geostrategisch als diplomatiek gebied en is de strategie een middel om de effecten van deze ontwikkelingen op de nationale belangen te verwerken. Juist in het cyberdomein is een dergelijke wisselwerking tussen nationale en internationale ontwikkelingen cruciaal. In lijn hiermee dient de internationale strategie complementair te zijn aan de bestaande nationale strategiedocumenten op deelterreinen, zoals de Nationale Cyber Security Strategie 2.0 en de Digitale Agenda.nl, die ook aspecten van internationaal beleid bevatten. Ook de beleidsinitiatieven die voortkomen uit de Global Conference on Cyberspace 2015 en de in 2011 mede door Nederland opgerichte Freedom Online Coalitie worden in de strategie meegenomen. Het uitgangspunt voor de Nederlandse inzet blijft de visie van een vrij, open en veilig internet. De Nederlandse inzet zal zich richten op de thema's economische groei en maatschappelijke ontwikkeling, internet governance, cybersecurity, internationale vrede en veiligheid in het cyber domein, digitale rechten, bestrijding van cybercrime en capaciteitsopbouw. Het kabinet wil de sterke uitgangspositie van Nederland op deze terreinen verder versterken en benutten voor de behartiging van nationale belangen en versterking van de internationale rechtsorde.

De internationale strategie vormt de visie van Nederland op internationale samenwerking in het digitale domein. Beleidsontwikkeling en -uitvoering op de verschillende deelterreinen blijft onder verantwoordelijkheid van de relevante departementen.

3.2 Coalitievorming

De WRR beveelt in zijn advies aan tot een verbreding van het diplomatieke werkveld. Deze inspanning zou er m.n. op gericht moeten zijn de zogenaamde «swing states» ervan te overtuigen dat het beschermen van het internet een belang van alle staten is.

Het digitale domein is een relatief nieuw beleidsterrein waar internationaal nog weinig in de vorm van afspraken, conventies of verdragen is vastgelegd, en waarop zowel publieke als private actoren actief zijn en nieuwe machtsverhoudingen ontstaan. We kunnen er niet langer vanuit gaan dat dat de post-1945 wereldorde doorslaggevend zal zijn bij de uitwerking van nieuwe vormen van samenwerking en ordening.

In vrijwel alle internationale discussies over het digitale domein is er sprake van een scherpe tegenstelling tussen enerzijds de multistakeholder-georiënteerde landen waaronder Nederland, die pleiten voor bescherming van de integriteit van het internet, en anderzijds de meer staatsgeoriënteerde landen die pleiten voor controle en inperking van datgene dat over het internet wordt verspreid. Tussen deze kanten van het spectrum bevindt zich een grote groep landen die op basis van hun eigen politiek-economische en sociaal-maatschappelijke belangen nog geen duidelijk keuze heeft gemaakt; de zogenoemde «swing states». Het kabinet opereert geheel in lijn met dit advies van de WRR. Nederland wil *swing states* overtuigen dat zij op basis van deze nationale belangen baat hebben bij een vrij, open en veilig internet. Alleen als er voldoende steun is voor deze visie op internet kan met vertrouwen worden gewerkt aan bijvoorbeeld internationale overeenkomsten op het gebied van cyber. Tot op heden is deze coalitie van landen te klein.

Nederland investeert op drie manieren in het versterken van coalities:
- Verbreden van deelname van landen / bedrijven aan internationale discussies over cyber issues;
- Versterken van publiek-private samenwerking en multistakeholder besluitvorming zodat overheden, bedrijven, civil society, de technische gemeenschap en academici wereldwijd kunnen deelnemen aan voor hen relevante overleggen over cyber;
- Opbouw van kennis en kunde over cyber in derde landen zodat deze in staat worden gesteld om de visie van een vrij, open en veilig internet te implementeren

Zo heeft Nederland gezorgd voor een brede geografische vertegenwoordiging tijdens de GCCS2015, zodat landen die de *internetboom* ondervinden, betrokken worden in de discussies rond internet governance, veiligheid en privacy. Daarnaast is een goede geografische balans ook een voortdurend aandachtspunt in de door Nederland opgerichte Freedom Online Coalitie.

Nederland ziet capaciteitsopbouw als een instrument om de dialoog met *swing states* die lijden onder een gebrek aan capaciteit, beleid of strategie te faciliteren. Door bij te dragen aan het versterken van capaciteiten van landen op het gebied van cybersecurity en cybercrime kunnen grensoverschrijdende digitale dreigingen beter worden aangepakt. Het Global Forum on Cyber Expertise (GFCE) is een belangrijk nieuw instrument om cybercapaciteiten wereldwijd te versterken. Het GFCE is een informeel platform waar landen, bedrijven en internationale organisaties in samenwerking met *civil society* initiatieven kunnen opzetten om de digitale kloof te overbruggen. Zo werkt Nederland bijvoorbeeld samen met Senegal aan cybersecurity strategieën voor West-Afrika. Ook gaat het GFCE versnippering tegen door als platform initiatieven die wereldwijd lopen bij elkaar te brengen.

Naast de interstatelijke relaties, zijn vertegenwoordigers uit het maatschappelijk middenveld belangrijke coalitiepartners bij het streven naar een vrij, open en veilig internet en bij de bevordering van het multistakeholder model dat alle relevante stakeholders de mogelijkheid biedt een rol te spelen bij de besluitvorming. In internationale besluitvormingsprocessen is er echter vaak geen plaats voor niet-statelijke actoren op het moment dat er afspraken worden gemaakt over de regulering en de toekomst van het internet. Nederland faciliteert en stimuleert de rol van civil society – NGOs, technische gemeenschap en academici – om cyberdebatten «inclusiever» te maken.

Tijdens de GCCS heeft Nederland bijvoorbeeld een belangrijke inspanning gedaan om te zorgen dat een brede groep vertegenwoordigers vanuit civil society aanwezig was door middel van een tweedaagse capaciteitsopbouwtraining voorafgaand aan de conferentie en financiële ondersteuning voor deelname van civil society vertegenwoordigers, met name uit de Global South. Eenzelfde inspanning deed Nederland recent in aanloop naar de tweede onderhandelingsronde van de review van de World Summit on the Information Society +10 Process. Nederland financierde in New York een tweedaagse bijeenkomst om ervoor te zorgen dat vertegenwoordigers uit ontwikkelingslanden ook in New York konden meepraten over deze VN agenda en hun input op het slotdocument konden coördineren.

Daarnaast consulteert de Nederlandse overheid (inter)nationale NGOs bij zijn standpuntbepaling in diverse (inter)nationale trajecten zoals het Internet Governance Forum, ICANN, de onderhandelingen over de World Summit on Information Society (WSIS+10), en tijdens Freedom Online Coalition (FOC) consultatiesessies. Onder het voorzitterschap van Nederland van de FOC werkgroep «An Internet Free and Secure» wordt gewerkt aan een nieuwe vorm van samenwerking tussen staten (Nederland, Canada en de VS), bedrijven en civil society. Deze werkgroep biedt een uniek platform voor een open en eerlijke dialoog over cyber gerelateerde onderwerpen, met de aanbevelingen over hoe samenwerking op (inter)national niveau structureel kan worden vormgegeven als waardevolle uitkomst van dit initiatief.

3.3 Verschillende vormen van veiligheid en rolverdeling tussen actoren

Veiligheid en vertrouwen zijn basisvoorwaarden voor burgers, bedrijven en overheden om van het internet gebruik te kunnen maken. De WRR roept op om verschillende vormen van veiligheid op het internet van elkaar te onderscheiden en de verantwoordelijkheden en taken van de verschillende actoren duidelijk af te bakenen. Er zijn vele verschillende vormen van veiligheid. Beide rapporten noemen: economische veiligheid, bescherming tegen (cyber)criminaliteit, consumentenbescherming, informatieveiligheid, van informatie en informatiegaring, het beschermen van nationale veiligheid door het voorkomen van maatschappelijke ontwrichting, en diverse vormen van ICT veiligheid waaronder met name beschikbaarheid, vertrouwelijkheid en integriteit.

Het kabinet voert de volgende taken uit: investeren in bewustzijnsvergroting, weerbaarheid en nationale cybersecurity, detectie, opsporing en vervolging, respons, diplomatie, en bevorderen van internetvrijheid en internationale veiligheid. Deze taken zijn bij verschillende onderdelen van de rijksoverheid en bij uitvoeringsorganisaties belegd, zoals het Nationaal Cyber Security Centrum (NCSC) dat onder het Ministerie van Veiligheid en Justitie valt, de inlichtingen- en veiligheidsdiensten, opsporingsdiensten, verschillende ministeries die verantwoordelijkheid dragen voor onderdelen van de kritieke infrastructuur in Nederland, de Ministeries van Buitenlandse Zaken, Defensie, Veiligheid en Justitie en Economische Zaken en het Ministerie van Binnenlandse Zaken voor de bedrijfsvoering van het Rijk en waarborging van mensenrechten. De WRR gaat in deze context specifiek in op de rolverdeling tussen de Computer Security Incident Response Teams en inlichtingen- en veiligheidsdiensten.

Hierbij moet worden opgemerkt dat cyberdreigingen in de praktijk vaak meerdere van de hier genoemde dimensies omvatten, waardoor het volledig scheiden van domeinen lastig of onwenselijk is. Zo is het werk van de I&V diensten gericht op het beschermen van de nationale

veiligheid, bijvoorbeeld door onderzoek te doen naar spionage en sabotage in het digitale domein. De daaruit verkregen dreigingsinformatie kan uiteindelijk echter ook de individuele digitale weerbaarheid van bedrijven en burgers ten goede komen. Zo hebben AIVD en MIVD nieuwe en meer geavanceerde dreigingen en aanvallen vaak eerder in het vizier dan andere partijen, omdat zij als enige de wettelijke taak en de wettelijke bevoegdheden hebben van de Wet op de Inlichtingen en Veiligheidsdiensten 2002. De trends worden integraal beschreven in het jaarlijkse Cyber Security Beeld Nederland (CSBN) en daarmee voor iedereen beschikbaar. De diensten werken samen met het NCSC in het Nationaal Detectie Netwerk waarbinnen de bevindingen, zoals nog onbekende *Advanced Persistent Threats* en bijbehorende *signatures*, waar mogelijk worden gedeeld met publieke en private partners om hun weerbaarheid te verhogen.

Daar waar verschillende vormen van veiligheid bij elkaar komen en de belangen niet volledig overeenkomen, maakt het kabinet een afweging om zowel de nationale veiligheid als de individuele veiligheid van burgers en bedrijven zo goed mogelijk te beschermen. Door zowel AIV als WRR wordt het dilemma aangehaald waarmee de overheid wordt geconfronteerd rondom het gebruik van encryptie. Encryptie is enerzijds van belang voor de systeem- en informatiebeveiliging en de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Anderzijds kan het de staat belemmeren bij het uitvoeren van zijn verantwoordelijkheid om ernstige misdrijven op te sporen en de nationale veiligheid te beschermen. Het recentelijk verschenen kabinetsstandpunt encryptie is een helder voorbeeld van de soort van afweging die het kabinet maakt bij het streven naar een internet dat open, vrij en veilig is. In het standpunt wordt geconcludeerd dat het kabinet «[t]ot taak [heeft] de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie. Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen uitdragen.»[11]

Indien nodig (bijvoorbeeld in geval van crisis) worden ook de verschillende veiligheidsorganisaties samengebracht. Het Ministerie van Veiligheid en Justitie heeft hierbij een coördinerende verantwoordelijkheid. Het NCSC is het nationaal kennis- en expertise centrum op het gebied van digitale veiligheid en de CERT voor de rijksoverheid en vitale sectoren. Samen met zijn partners binnen de overheid (onder andere de Nationale Politie, de AIVD en het Ministerie van Defensie waaronder de MIVD), wetenschap en bedrijfsleven zorgt het NCSC ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft conform het wetsvoorstel «Gegevensverwerking en meldplicht cybersecurity»[12].

---

[11] Kamerbrief over kabinetsstandpunt encryptie, Kamerstuk 26 643, nr. 383, 4 januari 2016.

[12] «Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)», Kamerstuk 34 388, voorstel van wet gepresenteerd 21 januari 2016.

4. Reactie op deeladviezen AIV

4.1 Dataprotectie

Internetgebruikers moeten er op kunnen vertrouwen dat overheden en organisaties hun data en persoonsgegevens goed beschermen. Uitgangspunten bij het ontwikkelen van beleid en wet- en regelgeving voor dataprotectie in de EU zijn het vertrouwen van de gebruiker, transparantie, een risico-georiënteerde benadering en beperkte regeldruk voor aanbieders van internetdiensten. Vanuit die positie voert het kabinet ook het debat in Europa over diverse dataprotectie-instrumenten, zoals de Algemene verordening gegevensbescherming, de richtlijn gegevensbescherming opsporing en vervolging en het onlangs door de Europese Commissie gesloten – en nog nader uit te werken – akkoord met de Verenigde Staten over de opvolger van het Safe Harbor verdrag.

Het kabinet hecht groot belang aan rechtszekerheid rond internationale dataoverdracht en is dan ook verheugd dat de Europese Commissie op 2 februari bekend heeft gemaakt dat er een politiek akkoord is bereikt tussen EU en VS over een nieuw raamwerk voor de doorgifte van persoonsgegevens uit de Europese Unie naar de Verenigde Staten; het «EU-US Privacy Shield». De tekst moet nog uitgewerkt worden, wat naar verwachting nog tot juni zal duren. Alhoewel gedurende die periode de omstandigheden nog kunnen wijzigen, is Nederland positief over de verbeteringen die zijn aangebracht in termen van toezicht op de naleving en handhaving van de inhoud. Volgens de Commissie dient het nieuwe raamwerk een tweetal doelstellingen, namelijk de bescherming van de grondrechten van de EU-burgers en zekerheid voor het bedrijfsleven. Daarmee lijkt een einde te komen aan de onzekerheid bij het bedrijfsleven sinds oktober over de rechtmatigheid van dataopslag door internetbedrijven in de VS.

Een goede balans tussen commerciële belangen en privacy is belangrijk voor het vertrouwen van burgers in online diensten en voor economische groei. Respect voor privacy moet geen belemmerende factor zijn, maar een kader dat uitdaagt tot innovatief ondernemen en nieuwe diensten en toepassingen. Het vertrouwen in innovatieve diensten is een belangrijke voorwaarde voor de groei van de digitale economie. Een betere privacybescherming in de VS zou het internationale *level playing field* voor Europese technologiebedrijven ten opzichte van de grote spelers in de VS kunnen versterken. Nederland vertrouwt op de waarde van schriftelijk vastgelegde *representations* van de VS omtrent de waarborgen waarmee de rechtmatige toegang tot overgedragen gegevens, voor doeleinden verband houdend met de rechtshandhaving en de nationale veiligheid, zijn omringd. Nederland ziet de vervolgstappen met belangstelling tegemoet.

4.2 Economisch potentieel / vestigingsklimaat

Het kabinet is het met beide rapporten eens dat het internet voor de Nederlandse economie van groot belang is en dat Nederland een sterke internationale voorhoedepositie heeft veroverd, die onder meer valt af te lezen aan de hoge positie op verschillende internationale ranglijsten. Nederland beschikt over uitstekende netwerken, een goed opgeleide bevolking, een hoge internetpenetratiegraad en een toppositie in datacenters en internetknooppunten, inclusief intercontinentale danwel trans-Atlantische verbindingen. De Nederlandse economie is, naast die van het VK, de meest ICT-intensieve van Europa met een ICT-omzet die vijf procent van het BBP bedraagt, nog los van andere ICT-afhankelijke sectoren. Een kwart van de Nederlandse economische groei van de

afgelopen tien jaar komt voor rekening van ICT en 25 procent van de buitenlandse investeringen in Nederland is ICT-gerelateerd.

Het kabinet heeft de digitale economie over de volle breedte in haar beleid geïntegreerd om de ICT-gerelateerde groeipotentie veilig te stellen en uit te bouwen. In de kabinetsbrief[13] over de middellange termijnvisie op telecommunicatie, media en internet wordt uiteengezet hoe dit kabinet werkt aan de veiligheid, betrouwbaarheid en (internet)vrijheid in het digitale domein, met speciale aandacht voor:

- een interneteconomie die vrij is van oneigenlijke invloed van overheden, bedrijven en overige belangengroepen op de keuzevrijheid van gebruikers, zowel ter bescherming van burgerlijke vrijheden als ten behoeve van de (vrije) markt.
- de integriteit, continuïteit en bescherming van persoonsgegevens als basis voor vertrouwen in data- gedreven markten.

In de Digitale Agenda.nl; ICT en Innovatie voor Economische Groei, (2011) en de Digitale Implementatie Agenda.nl (2011)[14] is uitgewerkt hoe het kabinet werkt aan het versterken van kansen voor economische groei, innovatie en ondernemerschap met internet en ICT. Voor de zomer zal een evaluatie en update van de Digitale Agenda naar de Tweede Kamer worden verzonden. Daarin wordt ook ingegaan op de motie Verhoeven van 15 oktober 2015,[15] waarin de regering wordt verzocht om de digitale infrastructuur te erkennen als derde mainport en een economische visie te ontwikkelen en uit te voeren om de positie van de digitale mainport te versterken.

Hiernaast wordt er specifieke aandacht geschonken aan de rol die ICT en internet kunnen bieden voor de nieuwe ontwikkelingen in alle sectoren, neem bijvoorbeeld de gezondheidszorg. De rol van internet en (big) data in de zorg wordt steeds groter en de kansen zijn groot. Door deze ontwikkelingen internationaliseert de zorg. Het is belangrijk dat data goed beveiligd zijn en de privacy van de patiënt wordt gegarandeerd. Door toegankelijke maar veilige data kunnen mensen meer regie op hun eigen gezondheid nemen, kunnen (mede door internationale dataverzameling) behandelmethodes verbeteren, kan de kwaliteit van zorg toenemen, kan een hogere mate van transparantie ontstaan en kan de deur geopend worden voor innovatieve technologische ontwikkelingen en producten.

Aan een positief vestigingsklimaat voor internetbedrijven wordt bijgedragen met een gericht stimuleringsbeleid voor de ICT- en internetsector. Zo is ICT een dwarsdoorsnijdend thema in het topsectorenbeleid, met een eigen Kennis- en Innovatie Agenda waarin NWO, TNO en EZ € 40 miljoen hebben gereserveerd voor ICT-gerelateerde Kennis en Innovatie in PPS-verband. In opdracht van het Ministerie van Economische Zaken wordt onderzoek verricht naar «Kansen voor de Cyber Security-sector in Nederland», waarin de bijdrage aan het ondernemingsklimaat voor de ICT-sector en het vestigingsklimaat vertrekpunt is voor beleidsaanbevelingen.

4.3 Rol en toezicht op I&V diensten

De AIV beveelt aan om effectief en onafhankelijk toezicht op de inlichtingen- en veiligheidsdiensten (I&V diensten) te verzekeren, alsmede de uitwisseling van gegevens tussen nationale inlichtingen- en veilig-

[13] Bijlage bij Kamerstuk 26 643, nr. 300.
[14] Kamerstuk 26 643, nr. 217.
[15] Kamerstuk 34 300 XIII, nr. 45.

heidsdiensten binnen Europa en daarbuiten van betere waarborgen te voorzien.

In de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002) wordt beschreven hoe er door diverse organen effectief en onafhankelijk toezicht wordt uitgeoefend op de taakuitoefening van de inlichtingen- en veiligheidsdiensten. Zoals bekend is op dit moment een herziening van de Wiv 2002 in voorbereiding. Bij die gelegenheid worden wederom de voorwaarden vastgelegd waaronder een inbreuk op grondrechten gerechtvaardigd wordt geacht. Het stelsel van toezicht moet immers ook na de herziening van de huidige Wiv 2002 voldoen aan de eisen die het Europese Hof voor de Rechten van de Mens stelt aan de activiteiten van de Inlichtingen- en veiligheidsdiensten die inbreuk maken op grondrechten.

Terecht wijst de AIV in de kabinetsreactie op het rapport van de Commissie Dessens waarin het kabinet aangeeft de aanbevelingen voor toezicht mee te wegen bij het opstellen van de nieuwe wet op de inlichtingen- en veiligheidsdiensten. Het gaat hierbij om het vinden van de juiste balans tussen het aan de ene kant aanpassen en op een aantal gebieden uitbreiden van de bijzondere bevoegdheden van de diensten en aan de andere kant het versterken van het stelsel van waarborgen, waaronder het toezicht. Op dit moment verwerkt het kabinet de reacties uit de internetconsultatie en de Privacy Impact Analyse in een nieuwe concept-wettekst, die voor het zomerreces aan de Afdeling advisering van de Raad van State zal worden aangeboden. Omdat de herziening nog in volle gang is acht het kabinet een specifieke bespreking van de nieuwe wet buiten de scope van deze reactie vallen.

Ten aanzien van de samenwerking met buitenlandse partnerdiensten hanteren de diensten diverse criteria, zoals de democratische inbedding van de betreffende dienst(en) en het mensenrechtenbeleid van het betreffende land. Deze criteria zijn belangrijke wegingsfactoren voor de intensiteit van de samenwerking met een partner. Deze werkwijze is in lijn met de aanbevelingen in toezichtsrapport 38 (2014) van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De criteria zullen ook worden vastgelegd in de herziene Wiv 2002.

4.4 Leidende rol van NL op EU dossiers

EU Voorzitterschap

Nederland ambieert een leidende rol als *digital gateway to Europe* en tevens als *safe place to do business and for people*. Tijdens het lopende Nederlands Voorzitterschap van Raad van de Europese Unie besteedt Nederland expliciet aandacht aan cybersecurity, cyber crime en digitale zaken zoals de Digital Single Market. Voortgang rond een vrij dataverkeer en internet governance (waarbij Nederland zich in zal zetten voor een vrij en open internet), en versterking van het kader voor grensoverschrijdende opsporing van cybercrime zijn daarbij prioriteiten.

In de *Friends of the Presidency Group on cyber issues (FoP)* besteedt Nederland aandacht aan de EU Cyber Security Strategie en bijbehorende Roadmap. Hierin komen onder andere de operationele samenwerking en informatie-uitwisseling, publiek-private samenwerking, *cyber diplomacy*, capaciteitsopbouw in landen buiten de EU, digitale rechten, het bestrijden van cyber-crime en *best practices op het gebied van* cybersecurity zoals *vulnerability disclosure* aan de orde. Nederland betrekt private partners in

het Nederlands Voorzitterschap, onder meer door de Cyber Security Raad een rol te geven bij de hoogambtelijke cyber security bijeenkomst in mei 2016.

Operationele samenwerking is ook een onderdeel van de Europese richtlijn voor Netwerk- en Informatiebeveiliging (NIB). De implementatie hiervan begint tijdens het voorzitterschap.

Exportcontrole dual-use ICT goederen en software

De AIV beveelt aan dat Nederland het Europees voorzitterschap in 2016 benut om voorstellen te ontwikkelen om verouderde wetgeving met negatieve effecten op internetvrijheid te actualiseren. In lijn hiermee en met de discussies tijdens de GCCS zal Nederland trachten tijdens het voorzitterschap de reeds lopende herziening van de EU Dual-Use Verordening aan te scherpen. Daarbij draait het om aanscherping van de controle op de export van dual-use surveillance technologieën. Een effectief en proportioneel exportcontrolebeleid is nodig om te voorkomen dat de EU surveillancetechnologie exporteert naar onderdrukkende regimes met ondermaatse waarborgen voor mensenrechten, die deze technologie in zouden kunnen zetten voor mensenrechtenschendingen. Nederland is zich bewust van de complexiteit van het formuleren van technische voorstellen op dit terrein en steunt dan ook het onderzoek wat thans plaatsvindt in opdracht van de Europese Commissie en kijkt uit naar het voorstel dat de Commissie zal presenteren op basis hiervan. Ook via andere multilaterale fora probeert Nederland deze visie internationaal te verankeren.

Netneutraliteit

Nederland was in de EU pionier met netneutraliteitswetgeving en heeft zich in de Europese netneutraliteitsdiscussie actief opgesteld op basis van de eigen nationale wetgeving. Zowel de Tweede Kamer, het kabinet als de (Nederlandse) Europarlementariërs hebben een rol gespeeld bij de totstandkoming van de Europese netneutraliteitsverordening. Verschillende Europese maatschappelijke organisaties (bijvoorbeeld ter bescherming van consumentenbelangen) hebben bij herhaling de Nederlandse praktijk en het Nederlandse standpunt uitgedragen.[16]

4.5. Dialoog met bedrijfsleven

Zoals het WRR-rapport en AIV-advies beschrijven is de relatie tussen de overheid en bedrijven tweeledig. Enerzijds zijn zij belangrijke partners bij het waarborgen van publieke belangen als privacy, veiligheid en vrijheid in het digitale domein, anderzijds kunnen sommige bedrijven daar, mede door hun wereldwijde dominante marktpositie, ook een negatieve invloed op hebben. Gezien de sleutelrol van vooral die laatste categorie bedrijven in het digitale domein, staat buiten twijfel dat zij serieuze diplomatieke aandacht verdienen.

De overheid werkt samen met het bedrijfsleven bij het verbeteren van de digitale vaardigheden en het benadrukken van de zorgplicht van bedrijven en overheden richting hun klanten. Ook ICT-producten en -diensten moeten veilig zijn. Bedrijven en overheden moeten aanspreekbaar zijn op hun verantwoordelijkheid. Ook moeten zij transparant zijn over wat ze in het kader van cybersecurity aan maatregelen nemen en hoe ze omgaan met de gegevens van gebruikers. Zoals in het Regeerakkoord gemeld stelt

[16] Zie hierover ook Kamerstuk 24 095, nr. 393.

het kabinet zich ten doel dat burgers en bedrijven hun zaken met de overheid digitaal en veilig kunnen afhandelen.

Alle departementen zijn voortdurend in dialoog met private partijen over een brede waaier van onderwerpen zoals: standpuntbepaling binnen ICANN en de ITU (EZ), afstemming in het jaarlijkse Nederlands Internet Governance Forum over internet governance in den brede (o.a. EZ, BZ, V&J, BZK), consultaties over de vormgeving van het beleid voor privacy, dataprotectie en de rol van intermediairs als bouwstenen voor de Europese digital single market (EZ), publiek-private samenwerking (V&J), en van normontwikkeling voor verantwoordelijk gedrag van staten in cyberspace tot capaciteitsopbouw en mensenrechten (BZ).

De rol, zorgplicht en ketenverantwoordelijkheid van private actoren, particulieren en overheid met betrekking tot veiligheid online is door het kabinet vastgelegd in NCSS 2.0 en ook de Cyber Security Raad houdt zich met dit vraagstuk bezig.